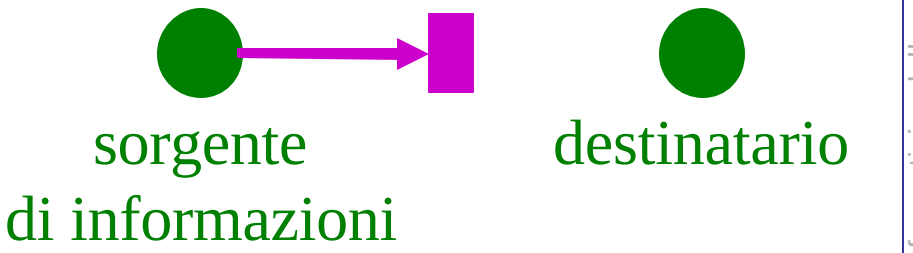
sicurezza delle reti

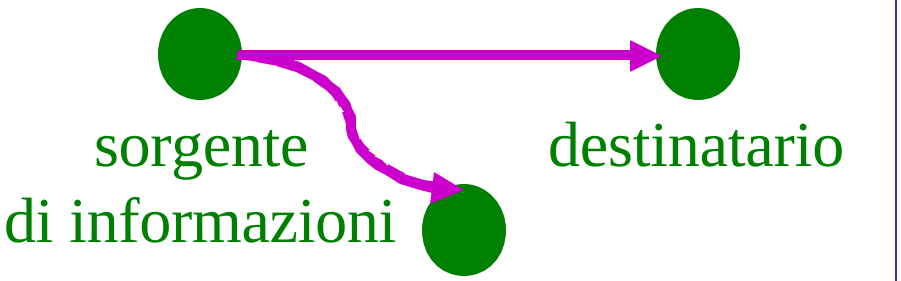
(metodi crittografici esclusi)

classificazione degli attacchi

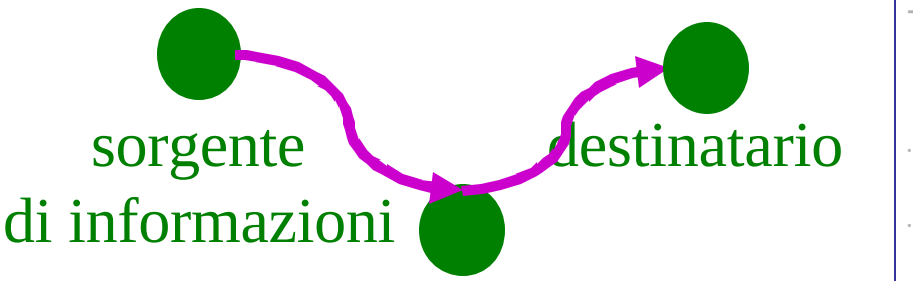
flusso normale



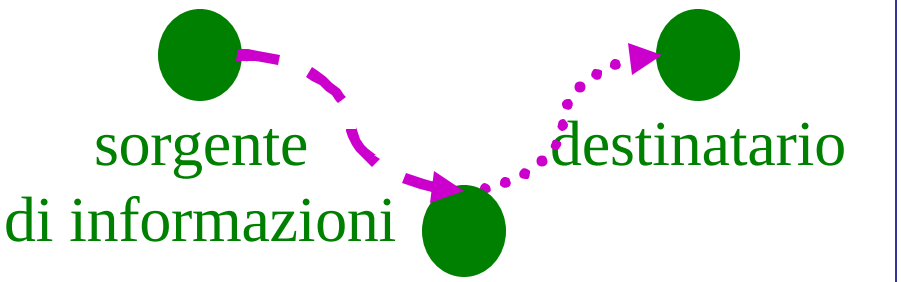
interruzione (DoS)



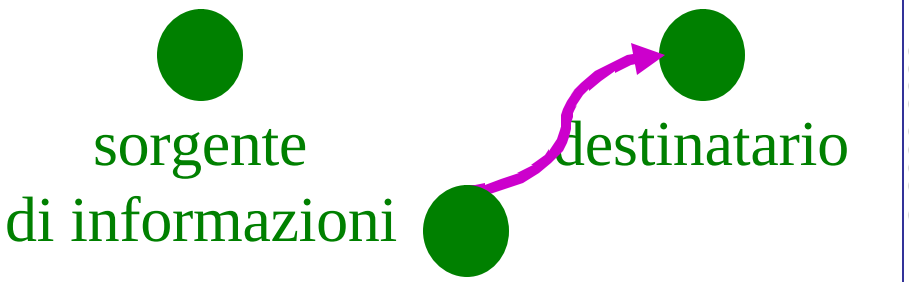
intercettazione (sniffing)



intercettazione (MiM passivo)



modifica (MiM attivo)



creazione (spoofing)

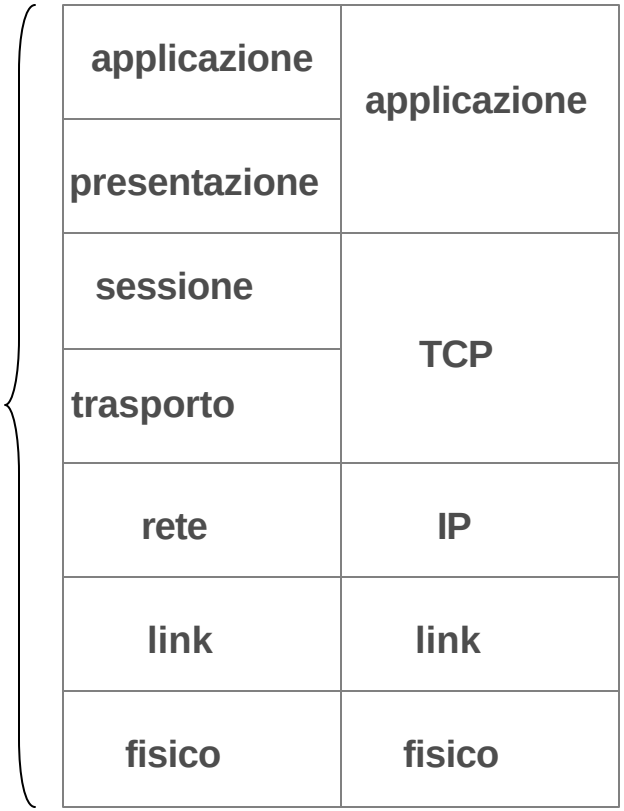
confinamento nelle reti

- il traffico è (o dovrebbe essere) ammesso solo tra sistemi e/o utenti con caratteristiche di sicurezza analoghe (principio di isolamento)
- esempi di classi di utenti
  - amministrazione
    - integrità e disponibilità: critiche per il business
    - confidenzialità: ciritica per legge
    - insieme di applicazioni ben definito
    - sistemi sotto controllo diretto
  - docenti
    - integrità e disponibilità: critiche per il business
    - confidenzialità: ciritica per certi aspetti particolari
    - richiesta alta flessibilità nelle applicazioni
    - il controllo dei sistemi è delegato ai gruppi di ricerca
  - studenti
    - best effort
    - sistemi non controllabili
  - utenti da internet di ricerca
    - servizi selezionati: web, email, siti di ricerca interni, login alle macchine di ricerca e a utenti da internet (altri)
    - servizi selezionati: web, email, siti di ricerca interni

la sicurezza nelle reti

vulnerabilità | **stack protocollare** | **contromisure**

DoS
Sniffing
MiM passivo
MiM attivo
spoofing



application
gateway, autenticazione
metodi crittografici

stateful firewall, ids,
metodi crittografici

screening router, ids
nat, metodi crittografici

vlan, conf. switch,
autenticazione, metodi crittografici

isolamento del mezzo
metodi crittografici

sicurezza del mezzo trasmissivo

- cavi rame
  - vulnerabilità
    - wiretapping
    - taglio
    - emissione elettromagnetica
  - contromisure
    - protezione fisica
    - wiretapping detection
- fibra
  - vulnerabilità
    - wiretapping
    - taglio
  - contromisure
    - protezione fisica
    - wiretapping detection

sicurezza del mezzo trasmissivo

- wireless
  - vulnerabilità
    - copertura “ad area” non “a presa”
      - impossibile stabilire chi riceve il traffico
    - area di copertura varia con la sensibilità delle stazioni
      - antenne fortemente direzionali possono ricevere hot spot molto lontani
    - facile avere utenti “parassiti”
    - DoS elettrmagnetico
      - non adatto a sistemi la cui disponibilità è critica
    - banda molto limitata
  - contromisure
    - per la confidenzialità e gli utenti parassiti: meccanismi crittografici a livello data link (più o meno efficaci)

livello data link

switch

- vulnerabilità
  - mac spoofing/flooding
    - impatto su arp, spanning tree, e livelli superiori
  - e altri problemi mitigabili: bugs del firmware, errori di configurazione
- contromisure
  - switch sofisticati permettono di rilevare e contrastare attacchi basati su mac spoofing
  - autenticazione
    - mac lock
    - web based
      - al primo accesso funziona solo dhcp e dns
      - lo switch fa da web server e tramite http chiede username e password
    - **802.1X**
  - isolamento
    - **VLAN**
      - vulnerabilità: GVRP è abilitato di default per standard e permette la configurazione automatica di vlan, oramai obsoleto e deletereo.

virtual lan vs. real lan

- le “forze” che guidano il progetto della rete fisica e delle vlan sono diverse
- rete fisica, cioè switch e cablaggio
  - ha come obiettivo la rete economicamente più conveniente che soddisfi i seguenti vincoli
    - piena connettività tra le prese
    - prestazioni richieste
    - vincoli ambientali (es. posizione spazi adibiti agli impianti)
    - vincoli tecnologici (es. lunghezza dei cavi)
    - normative (es. materiali non infiammabili)
    - affidabilità (se richiesta, es. resiste al fault di uno switch)
- vlan, cioè configurazione ideale “desiderata”
  - ha come obiettivo la migliore configurazione che soddisfi…
    - le specifiche funzionali
      - chi deve essere connesso con chi? vedi strutture organizzative che occupano l’edificio (es. dipartimenti, reparti, ecc)
    - le specifiche di sicurezza basate sulle classi di utenti (vedi isolamento)
    - facilità di gestione (es. ciascuna vlan un amministratore)

vlan

- su un singolo switch
  - ciascuna porta è associata ad una vlan
  - uno “switch virtuale“ per ciascuna vlan
- su più switch: 802.1Q
  - tra uno switch e l’altro i pacchetti viaggiano taggati con l’identificatore della vlan (802.1p)
- comportamenti caratteristici
  - confinamento di broadcast e unicast
    - switch di scarsa qualità (non standard) confinavano solo il broadcast (vulnerabile)
  - la comunicazione tra vlan deve avvenire attraverso un router proprio come tra lan distinte
- argomenti correlati
  - vlan asimmetriche, vlan per protocollo, GVRP, multiple spanning tree

livelli rete, trasporto e applicazione

vulnerabilità e minacce

- veicolo per attacchi ai sistemi
- elemento umano
  - email, web, ecc. l'utente permette l'entrata di virus, trojan, ecc.
- molte vulnerabilità già viste all'inizio del corso
  - protocolli in chiaro e non autenticati: necessari metodi crittografici
  - DoS, DDoS

firewalls

- apparecchiature che confinano (filtrano) selettivamente il traffico di rete
- network (layer3+4) vs. application (layer7)
  - network: stateful vs. stateless
- hardware vs. software
- personal fw vs. network fw

- possono avere altre funzionalità
  - nat, virtual private network, autenticazione utenti

soggetti, oggetti e diritti in un fw

- soggetto: un pacchetto/messaggio in ingresso
- oggetto: solo il firewall
- accesso: richiesta al firewall di essere instradato verso la destinazione
- diritti: per ciascun tipo di traffico in ingresso le destinazioni ammesse

- è un modo di vedere il fw molto concreto ma poco utile

il firewall come reference monitor

- un firewall può essere visto come un reference monitor di rete
  - soggetto: l'host sorgente che ha inviato il pacchetto/messaggio
  - oggetto: l'host destinazione che riceverà il pacchetto/messaggio
  - accesso: richiesta all'host destinazione di processare il pacchetto/messaggio inviato dall'host sorgente
    - la semantica vera (cioè l'effetto sull'host destinazione) dell'accesso è data dal protocollo di rete e dal contesto in cui viene usato: il fw non ha bisogno di conoscerla
  - diritti: categorie di traffico ammesso per la coppia di host

packet filter firewall

- basati sulla quadrupla <saddr,sport,daddr,dport>
- in pratica è un router + access control list

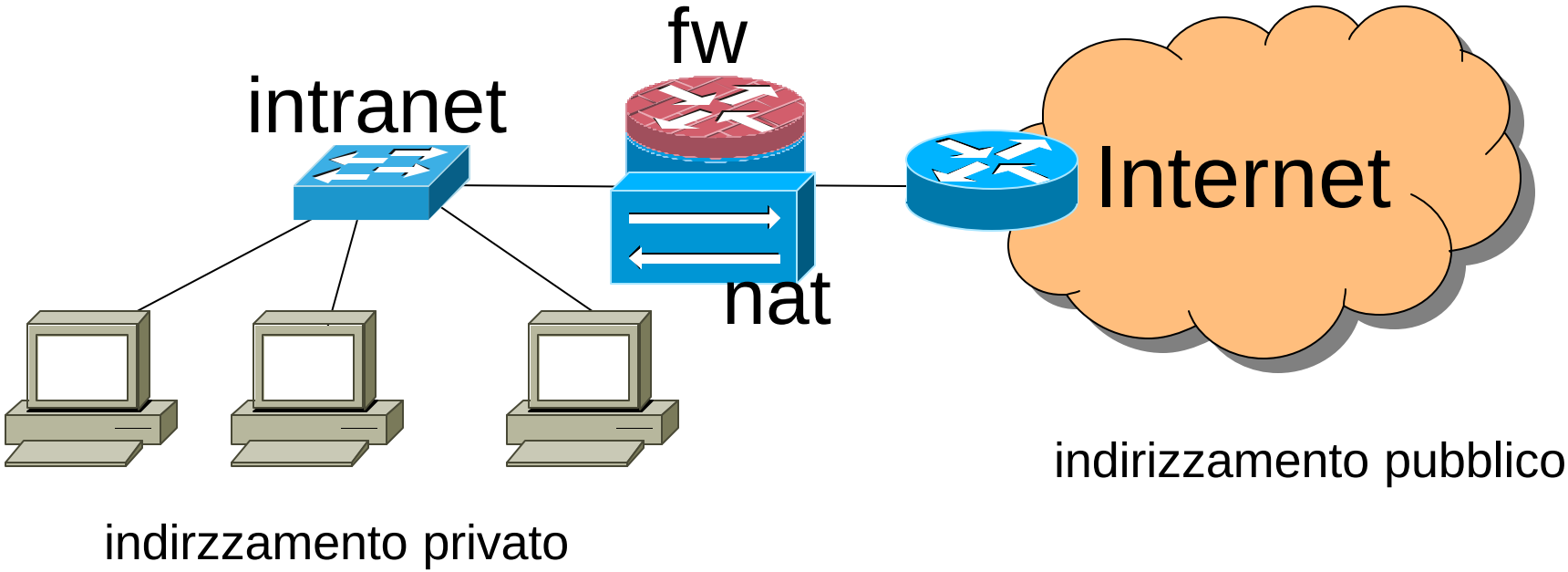
- detti anche “screening routers”

stateful packet filter firewall

- tengono traccia delle connessioni
  - solitamente tcp ma anche udp
  - stato della connessione: new, established, ecc.
- ciascun pacchetto è assegnato ad una connessione
  - filtrano in base allo stato della connessione
    - es. verso la rete interna solo se connessione è established
  - verificano la correttezza del protocollo
    - es. syn ammesso solo per connessioni nuove
  - permettono regole in base allo stato della connessione
- possono modificare il traffico
  - es. per implementare schemi anti-SYNflood

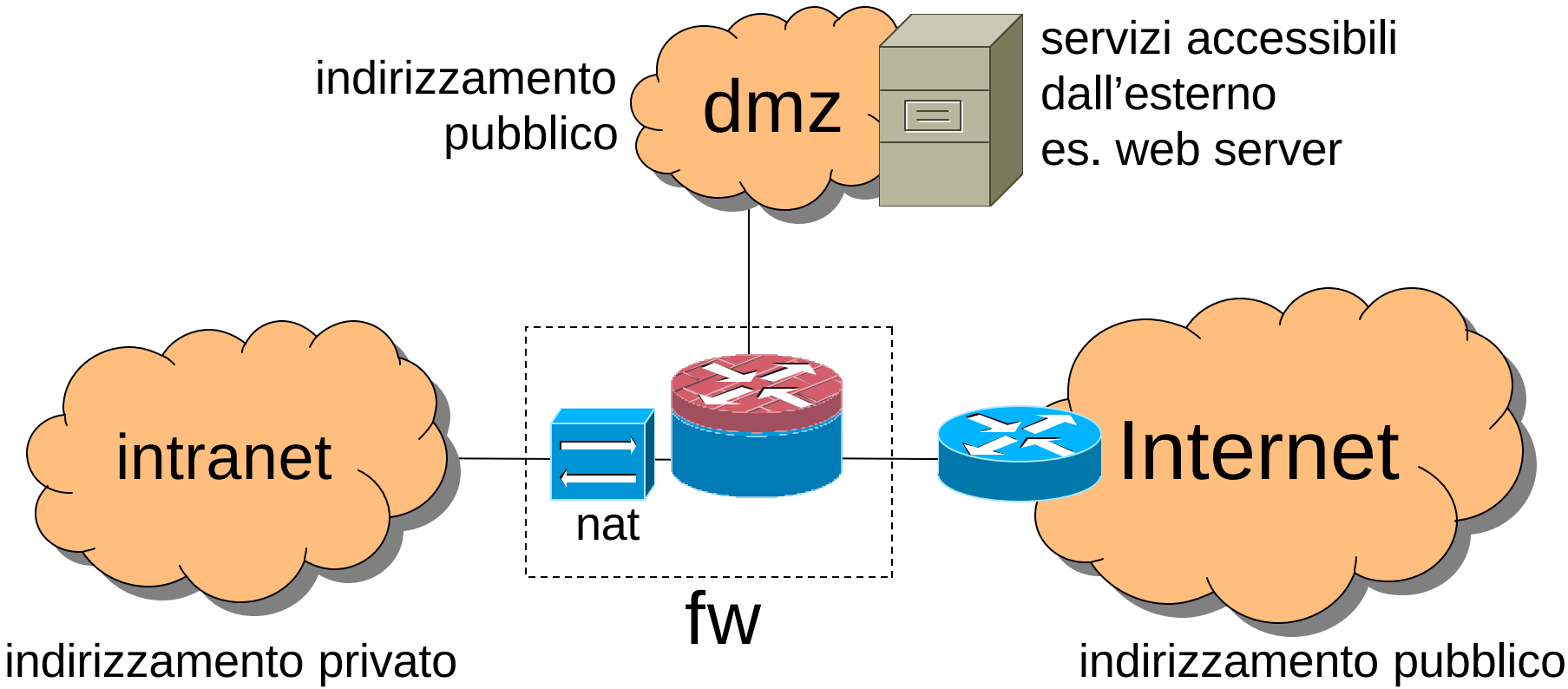
firewall, nat e intranet

- un semplice caso d'uso
  - isolare la intranet da Internet
  - in questa configurazione tipicamente il fw fa anche nat



dmz

- demiliterized zone (zona smilitarizzata) o perimeter network (rete perimetrale)
  - rete distinta sia da Internet che dalla intranet
  - gli host in tale rete sono in una classe di sicurezza distinta da quelli della intranet



dmz: esempio di policy

da \ a	host intranet	host dmz	host Internet
host intranet	all non si passa per il fw	richiesta dalla intranet si accede ai servizi della dmz	- dalla intranet non si accede a Internet
host dmz	risposta dalla dmz si risponde alle richieste della intranet	all non si passa per il fw	risposta dalla dmz si risponde alle richieste di Internet
host Internet	- da Internet non si accede alla intranet	richiesta da Internet si accede ai servizi della dmz	all non si passa per il fw

interpretazione per protocolli basati su tcp

- “richiesta”
  - un syn per una connessione NEW
- “risposta”
  - tutto ciò che è relativo ad una connessione ESTABLISHED (dopo il syn)

- facile da implementare in un firewall stateful

varianti

- intranet potrebbe dover accedere ad Internet
  - questo potrebbe rappresentare un grave problema di sicurezza perché Internet è una fonte di input non fidato
    - consigliato l'uso di application level gateway
- dmz potrebbe dover accedere a…
  - dns, per i log
    - fonte non fidata
  - servizi di altri fornitori
    - il grado di fiducia può variare

packet filtering: problemi

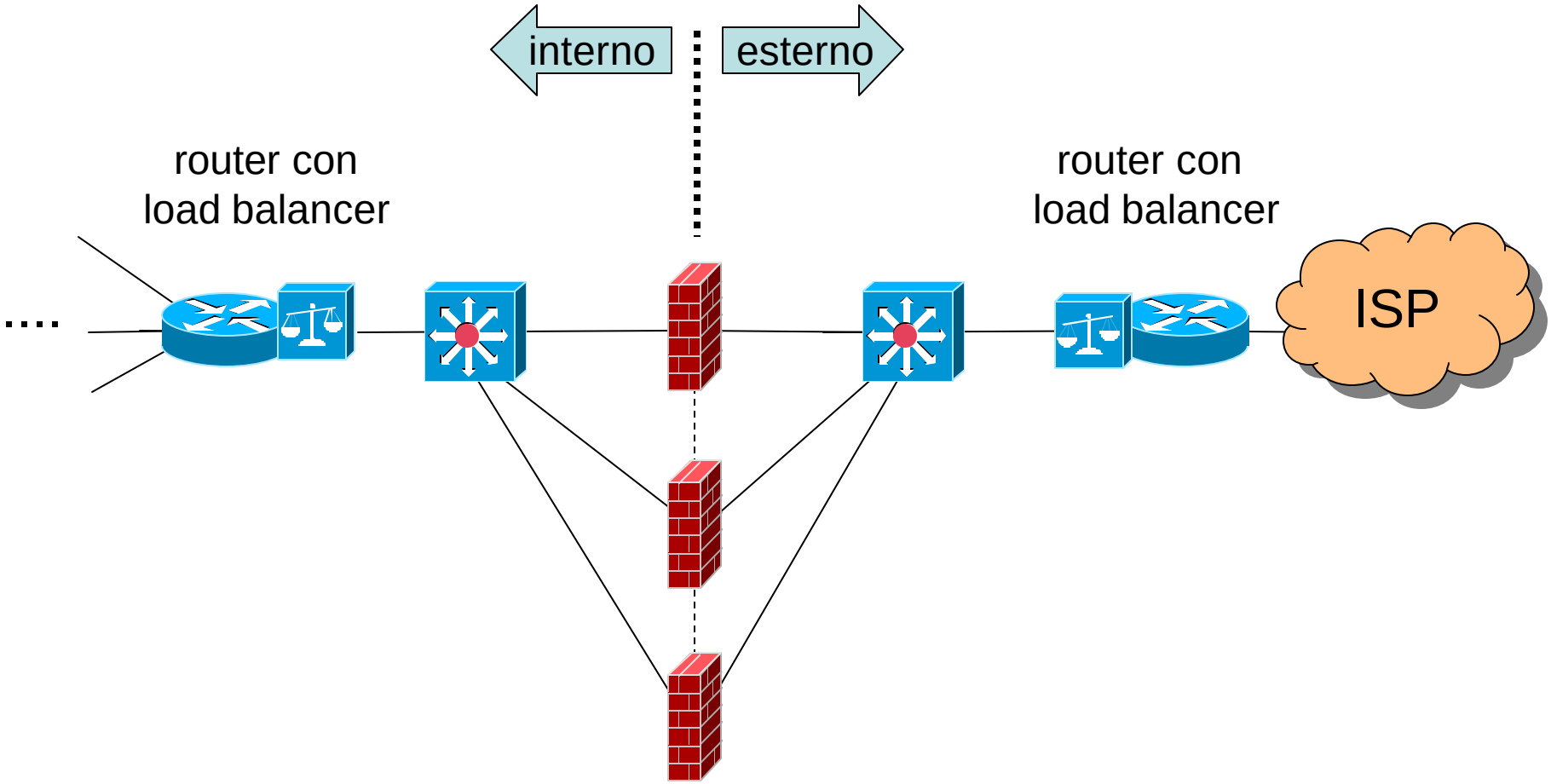
- la configurazione può essere molto complessa
  - facile fare errori
  - i firewall stateful sono un po' più semplici da configurare

prestazioni e affidabilità

- i fw spesso sono
  - un collo di bottiglia per le prestazioni
  - un single point of failure
- spesso utilizzati in configurazione “cluster” con tutti gli elementi attivi
  - bilanciamento del carico
  - ridondanza
- load balancer
  - semplice se i fw sono stateless
    - ciascun pacchetto assegnato ad un fw in maniera arbitraria (es. round robin)
  - fw stateful due possibilità:
    - load balancer assegna l’intera connessione ad un fw
      - non così ovvio: alcuni protocolli coinvolgono più sessioni tcp (es. ftp)
    - i fw si scambiano lo stato (soluzioni proprietarie)

prestazioni e affidabilità

- una architettura d'esempio

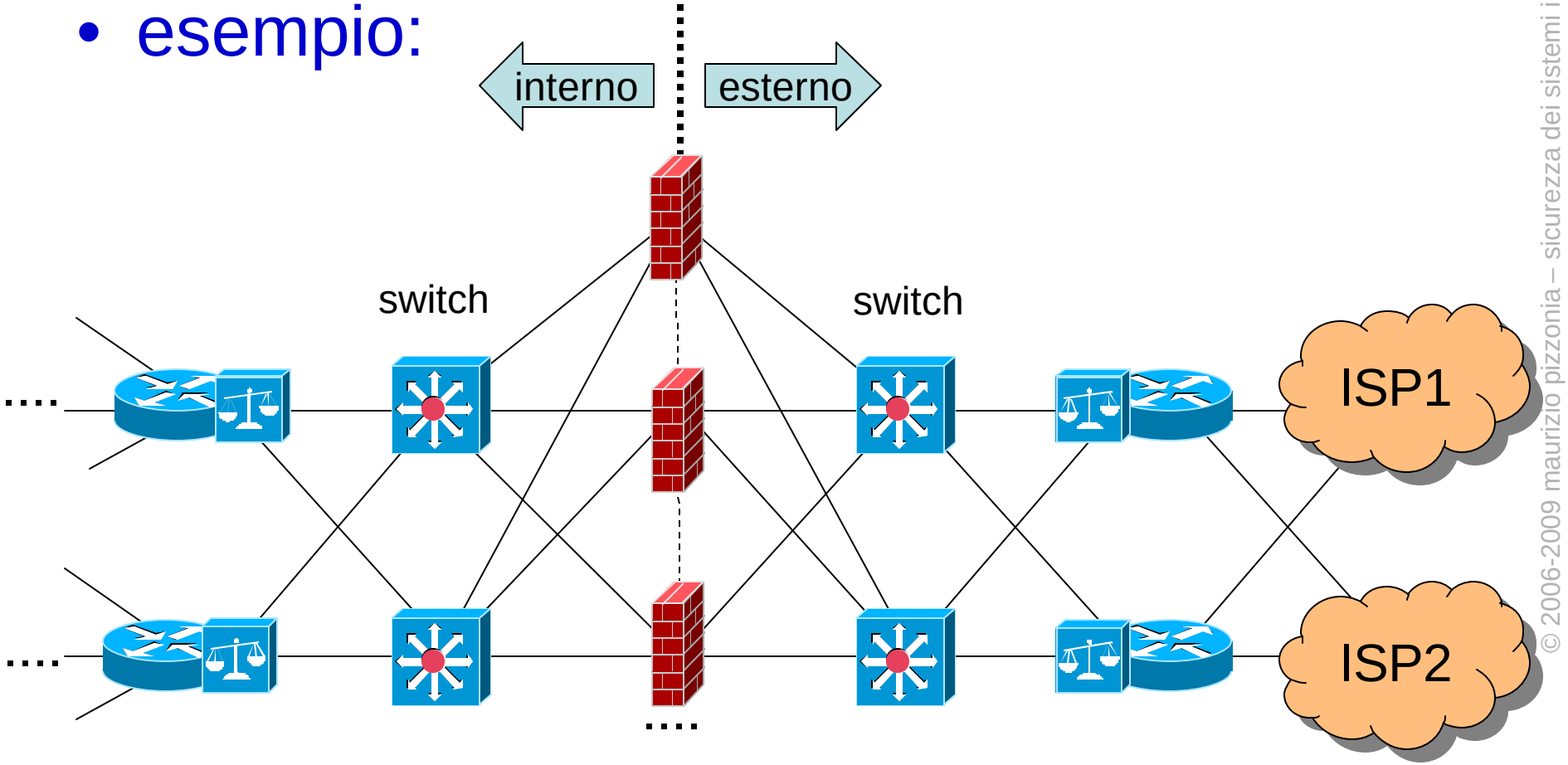


affidabilità dei componenti di contorno

- i router possono essere un single point of failure
  - quanto down-time siamo disposti a sopportare?
  - le configurazioni tolleranti ai guasti per mezzo di elementi ridondati si dicono in “fail over” o “high-availability”
- le configurazioni che prevedono tutti gli elementi ridondati possono essere molto complesse
  - costose
  - difficili da gestire
- high-availability è necessaria quando gli SLA (service level agreement) non prevedono il tempo per la sostituzione di uno degli elementi

full high-availability

- ciascun elemento dell'architettura deve essere ridondato
- esempio:



linux netfilter

- sistema di moduli Linux che realizza un fw
  - packet filter
  - stateful
  - nat
  - sistema di access list (chains) organizzate per funzionalità (tables)
  - tables
    - filter
      - chains: INPUT, OUTPUT, FORWARD
    - nat
      - chains: PREROUTING, POSTROUTING, OUTPUT
  - si possono definire delle “user-defined chain”
  - ciascuna tabella viene gestita da un modulo del kernel

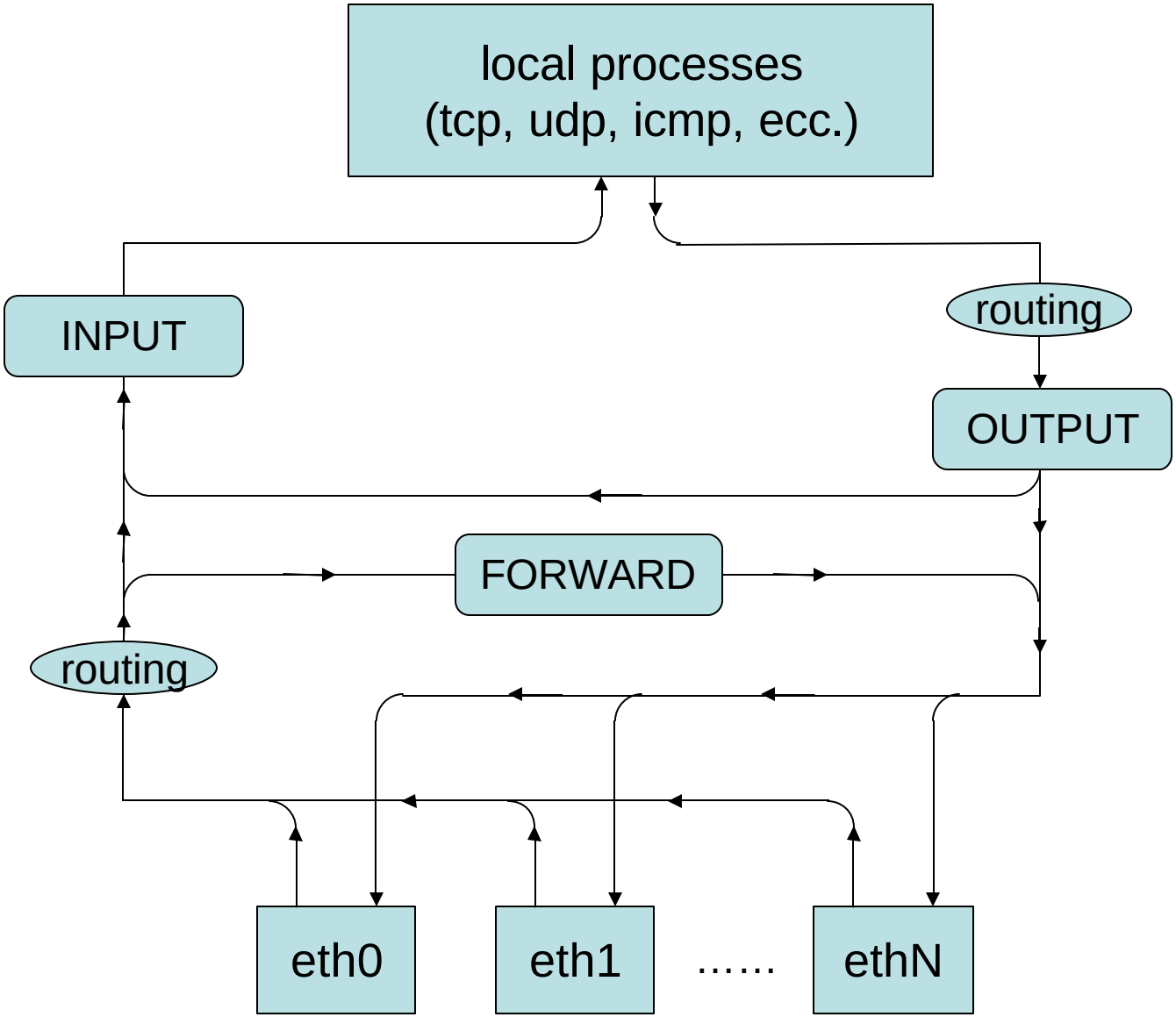
linux netfilter: chains (acl)

- ciascuna chain ha una sequenza di regole e un target
  - il target specifica cosa fare del pacchetto se questo non ha attivato alcuna regola
- target possibili
  - ACCEPT (pacchetto ok, lascia passare)
  - DROP (pacchetto droppato)
  - REJECT (come drop ma invia un icmp di errore al mittente)
  - <chain name> (salta alla chain specificata, come una chiamata a procedura, utile con “user-defined chain”)
  - RETURN (ritorna alla chain chiamante)
  - ...

linux netfilter: firewall rules

- una regola ha dei parametri e un target
  - i parametri specificano per quali pacchetti la regola viene attivata
  - il target specifica cosa fare
- parametri
  - protocollo (-p ip/tcp/udp/)
  - source/destination address (-s/-d [!]x.x.x.x/x)
  - source/destination port (--sport/--dport port)
  - input/output interface (-i/-o ethN)
  - tcp flags syn=1 e ack=0 (--syn)
  - e altri

linux netfilter: filter table



linux netfilter: connection tracking

- netfilter tiene traccia delle “connessioni”
  - per tcp e udp: coppia (non ordinata) di coppie {<addr, port>, <addr, port>}
  - per icmp echo: coppia di indirizzi {addr, addr}
- a ciascun pacchetto è associata una connessione (eventualmente ne viene creata una nuova)
  - questo viene fatto appena un pacchetto entra in netfilter da una interfaccia o dai processi locali
  - le connessioni muoiono per timeout o per protocollo (fin/ack, rst)
- stato del pacchetto
  - NEW: primo pacchetto della connessione
  - ESTABLISHED: pacchetto di una connessione già esistente
  - RELATED: nuova connessione associata ad una precedente (ftp, icmp errors)
  - INVALID: impossibile associare una connessione (es. icmp error non associati ad alcuna connessione)

linux netfilter: extended matches

- l'opzione -m <nome> permette di attivare molti altri tipi di regole
  - **state**: filtro in base allo stato (NEW, ESTABLISHED, RELATED, INVALID)
    - **conntrak** è una versione estesa
  - **mac**: filtro in base agli indirizzi mac di livello 2
  - **limit**: filtro in base alla frequenza di arrivo
    - anti DoS, anti scanning ecc.
  - **iprange**: es. 192.168.1.13-192.168.2.19
  - e molti altri

netfilter: comandi

- iptables
  - modifica e mostra la configurazione
    - -L mostra la configurazione
    - --flush cancella la configurazione
    - -A <chain> aggiunge in coda a <chain> un regola
    - ecc.
- iptables-save
  - dump della configurazione attuale
- iptables-restore
  - carica la configurazione da un dump fatto con iptables-save (più efficiente che molte chiamate a iptables)

esempio: nessun filtro

- **iptables --flush**
- **iptables-save**

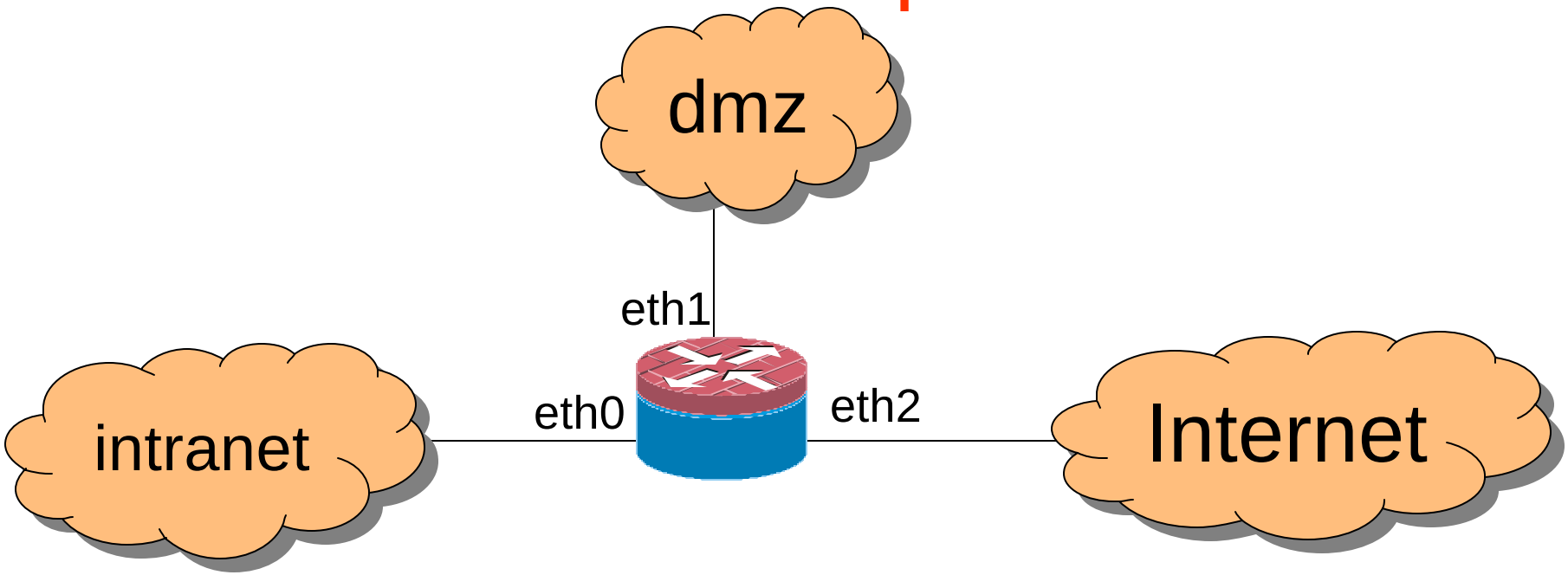
```
# Generated by iptables-save v1.3.3 on Fri Dec  8 17:58:19 2006
*filter
:INPUT ACCEPT [37:4620]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [19:1352]
COMMIT
# Completed on Fri Dec  8 17:58:19 2006
```

esempio: un semplice personal firewall

- **iptables -P INPUT DROP**
- **iptables -A INPUT -m state --state ESTABLISHED,RELATED –j ACCEPT**

```
# Generated by iptables-save v1.3.3 on Fri Dec  8 18:26:51 2006
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [14735:2397896]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Fri Dec  8 18:26:51 2006
```

implementazione della politica dmz di esempio




```
*filter
:INPUT ACCEPT [64:3448]
:FORWARD DROP [13:858]
:OUTPUT ACCEPT [409:37987]
-A FORWARD -i eth0 -o eth1 -m state --state NEW -j ACCEPT
-A FORWARD -i eth2 -o eth1 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

proxy applicativi

- sono detti anche application level gateways
- obiettivo (nell'ambito della sicurezza): verificare che i protocolli applicativi siano usati secondo la politica
  - la configurazione dei server è complessa, non sempre sotto controllo di esperti di sicurezza e non sempre i default sono sicuri
  - i protocolli applicativi sono complessi (es. http permette di modificare il sito web con "put") e molte loro caratteristiche sono pericolose
  - spesso un insieme molto ristretto di caratteristiche del protocollo è sufficiente alle esigenze
- devono conoscere i protocollo applicativo o almeno parte di esso
- due sessioni di trasporto
  - S $\leftrightarrow$ Proxy $\leftrightarrow$ D

proxy applicativi

- funzionamento
  - riceve una richiesta da una sorgente S per una destinazione D
  - la analizza per verificare che sia conforme a certe regole
  - riproduce la richiesta ponendo se stesso come sorgente
  - ottiene la risposta da D la analizza per verificare che sia conforme a certe regole
  - riproduce la risposta per S
- poiché devono processare in maniera sicura dati non fidati sono detti “bastion hosts”
- se l’analisi del protocollo è sofisticata vengono detti “guard”

web proxy: obiettivi

- **controllo di accesso al servizio, autenticazione, test per codice malevolo**
- anonimità
- prestazioni: caching
- modifica contenuto
  - censura
  - riformattazione per schermi piccoli (cellulari, PDA)
- reverse proxy: un proxy in prossimità di un web server che riceve le richieste da Internet
  - sicurezza (bastion host), load balancing, encryption acceleration, cache del contenuto statico
- open source: squid, privoxy, spikeproxy

transparent web proxy

- un web proxy regolare richiede la configurazione del browser
  - scomodo
  - la presenza del proxy è palese
- un proxy “transparent” intercetta richieste http qualsiasi
  - non richiede configurazione del browser
  - il proxy c’è ma non si vede

web proxy: vulnerabilità

- il protocollo http prevede il metodo CONNECT
- tale metodo viene interpretato dai proxy come un comando per lasciare passare connessioni arbitrarie
  - usato per connessioni http criptate
    - https (http su secure socket layer)
  - se connessione è criptata il proxy non può conoscerne il contenuto
- disabilitare CONNECT comporta l'impossibilità di usare https

mail proxy

- i mail transfer agent sono in sostanza dei mail proxy
  - hanno smtp sia come input che come output
  - obiettivi:
    - virus, spam
  - open source: exim, qmail, spamassassin, smtp.proxy
- protocolli pop3 e imap
  - open source: pop3.proxy, imap proxy

proxy: altre applicazioni

- ftp
  - open source: www.ftpproxy.org
- dns
  - un name server agisce da proxy quando server richieste ricorsive
  - open source: bind
- sql
  - open source: sqlrelay

circuit-level proxy

- sono dei proxy generici che operano su sessioni tcp
  - non conoscono alcun protocollo applicativo
- uso tipico: dare accesso a client/utenti specifici nella rete interna a server specifici in Internet
- possono prevedere autenticazione
- richiede un supporto esplicito del client
- implementazione tipica: SOCKS
  - rfc 1928

network based IDS (NIDS)

- verifica la presenza sulla rete di traffico riconducibile ad attività sospette
- si avvale di uno sniffer
  - particolari precauzioni per reti switched
- riconosce il traffico malevolo tramite
  - regole contenuto in un db
  - tecniche statistiche per anomaly detection
- open source: snort (http://www.snort.org/)
  - supportato sia sotto Windows che sotto Linux

NIDS: azioni

- può generare un log delle attività sospette
- può riconfigurare automaticamente un firewall
  - attività di contrasto automatica
  - detti anche intrusion prevention systems (IPS)
  - un NIDS–IPS è tipicamente in configurazione in-line con firewall incorporato
    - in sostanza un firewall con due interfacce che analizza il traffico da cui è attraversato

NIDS e connessioni tcp

- un NIDS non si può limitare a verificare ciascun pacchetto ip
- gran parte degli attacchi sono a livello applicativo e incapsulati in tcp
- è necessario seguire la sessione tcp e applicare le regole al flusso di bytes
  - molto oneroso!

NIDS: scalabilità

- un NIDS dovrebbe essere in grado di elaborare tutto il traffico della rete
  - ogni pacchetto un lookup nel db
    - db in memoria
  - perdita di pacchetti $\rightarrow$ perdita di accuratezza
    - falsi negativi
  - le risorse necessarie dipendono da
    - numero di pacchetti
    - quantità di flussi tcp e desequenziamento

HIDS vs. NIDS

- controllano aspetti diversi
  - host based
    - legittimtà del comportamento del software (integrità del sistema)
    - legittimità del traffico di rete da/per un host specifico
  - network based:
    - legittimità di tutto il traffico nella rete
- approcci complementari

NIDS: load balancing

- è possibile mettere più NIDS in parallelo
- è necessario che ciascun flusso venga analizzato dallo stesso NIDS
  - flusso: pacchetti con la stessa quadrupla <saddr, sport, daddr, dport>
    - altra definizione di flusso possibile: stessa coppia <saddr, daddr>
  - in questo modo ciascun NIDS mantiene un insieme di connessioni tcp

Unified Threat Management (UTM)

- evoluzione del concetto di firewall
- unisce molte delle funzionalità
  - firewall
  - network intrusion prevention
  - sicurezza delle email
    - antivirus, anti-spam
  - VPN
  - content filtering
  - load balancing
- semplicità di gestione e riduzione dei costi